INFORMATION AND CONTROL **10**, 378–385 (1967)

Cyclic Error-Locating Codes

J.-M. GOETHALS

M.B.L.E. Research Laboratory, Brussels, Belgium

A new class of error-locating codes, which are equivalent to cyclic codes, is presented, together with a general decoding procedure. Connections with some previously considered error-locating codes are pointed out.

LIST OF SYMBOLS

C'	= error-detecting code
C''	= error-correcting code
C	= error-locating code
H', H'', H	= parity check matrices for the codes C', C'', and C, respectively
n', n'', n	= block lengths of the codes C', C'', and C, respectively.
d	= number of detectable errors
t	= number of correctable errors
E_d	= class of detectable errors
E_t	= class of correctable errors
$g(x)$	= generating factor for the code C'
$G(x)$	= generating factor for the code C''
$GF(q)$	= Galois field with q elements
S_i	= ith component of syndrome
α, β, γ	= primitive roots of unity (nth, n'th, n''th, respectively).

Wolf and Elspas (1963), Chang and Weng (1965), and Wolf (1965) have introduced a new class of codes called "error-locating" (EL codes), with properties intermediate between error-detecting and error-correcting codes. The words in these codes are supposed to be divided into n'' subwords each of length n', the total block length being thus $n = n'n''$. If errors belonging to a class of patterns E_d occur within subwords, and if the erroneous subwords form a pattern of errors belonging to a class E_t, then the errors are detected and the erroneous subwords are located.

This paper describes a new class of error-locating codes constructed by

means of cyclic codes. The resulting codes are shown to be equivalent to cyclic codes under coordinates permutation, and allow implementation with the well-known techniques used for cyclic codes. A general decoding procedure is presented. In addition, equivalence of some of the Wolf-Elspas codes with ours has been established.

A NEW CLASS OF ERROR LOCATING CODES

The main result is stated in the following theorem.

THEOREM. *Let C' of block length n' be a cyclic d-error-detecting code generated by the product*

$$g(x) = g_1(x)\, g_2(x) \cdots g_r(x) \tag{1}$$

of r distinct irreducible factors over $GF(q)$, and let $GF(q^m)$ be the smallest extension field of $GF(q)$ containing all the roots of $g(x)$.

Let C'', of block length n'' relatively prime to n', be a cyclic t-error-correcting code generated by the product

$$G(x) = G_1(x)\, G_2(x) \cdots G_s(x) \tag{2}$$

of s distinct irreducible factors over $GF(q^m)$, and let $GF(q^{mp})$ be the smallest extension field of $GF(q^m)$ containing the $n'n''$th roots of unity.

Then there exists an E.L. Code C of block length $n = n'n''$ and having not more than rspm check digits over $GF(q)$, which locates up to t erroneous subwords, each subword having not more than d errors. Furthermore, C is equivalent to a cyclic code.

PROOF. Let β_i be any root of $g_i(x)$, and similarly let γ_i be any root of $G_i(x)$. Then, the following matrices

$$H' = \begin{bmatrix} 1 & \beta_1 & \beta_1^2 & \cdots & \beta_1^{n'-1} \\ 1 & \beta_2 & \beta_2^2 & \cdots & \beta_2^{n'-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \beta_r & \beta_r^2 & \cdots & \beta_r^{n'-1} \end{bmatrix} \tag{3}$$

$$H'' = \begin{bmatrix} 1 & \gamma_1 & \gamma_1^2 & \cdots & \gamma_1^{n''-1} \\ 1 & \gamma_2 & \gamma_2^2 & \cdots & \gamma_2^{n''-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \gamma_s & \gamma_s^2 & \cdots & \gamma_s^{n''-1} \end{bmatrix} \tag{4}$$

may be taken as parity check matrices[1] for the codes C' and C'', respectively. We shall show that the Kronecker product of the matrices

[1] For a more detailed account of the theory of cyclic codes, the reader is referred to Peterson (1961).

H'' and H'

$$H = H'' \times H' = \begin{vmatrix} H' & \gamma_1 H' & \cdots & \gamma_1^{n''-1} & H' \\ H' & \gamma_2 H' & \cdots & \gamma_2^{n''-1} & H' \\ \vdots & \vdots & & \vdots & \vdots \\ H' & \gamma_s H' & \cdots & \gamma_s^{n''-1} & H' \end{vmatrix}; \tag{5}$$

where the product is to be computed in GF(q^{mp}) may be taken as parity check matrix for the desired EL code.

The matrix (5), where the elements are considered as elements of $GF(q^{mp})$, has rs rows and $n = n'n''$ columns. The syndrome[1] is considered to be an rs-component vector, each component being an element of $GF(q^{mp})$. Let errors occur in the subwords numbered $j_1, j_2, \cdots j_t$, and let the corresponding error patterns be described by the vectors $v_{j_1}(x), v_{j_2}(x), \cdots v_{j_t}(x)$. Then, the ith component of the syndrome, with $i = ri'' + i'$, is

$$S_i = \sum_{k=1}^{t} (\gamma_{i''})^{j_k} v_{j_k}(\beta_{i'}). \tag{6}$$

If not more than d errors occurred in the j_kth subword, the corresponding vectors

$$v_{j_k}(\beta_{i'}) \quad \text{for} \quad i' = 1, 2, \cdots r \tag{7}$$

belonging to $GF(q^m)$ cannot be simultaneously zero, since C' is d-error-detecting. On the other hand, any $2t$ or fewer columns of H'' are linearly independent over $GF(q^m)$, since C'' is t-error-correcting. As a consequence, errors occurring in distinct sets of not more than t subwords cannot give the same syndrome, since otherwise $2t$ or fewer columns of H'' would be dependent over $GF(q^m)$. Distinct sets of erroneous subwords, giving distinct syndromes, may thus be located with the parity-check matrix (5) which has at most $rsmp$ independent rows over $GF(q)$.

We next show that the resulting code is equivalent to a cyclic code. Since n' and n'' are relatively prime, we may write[2]

$$a\,n' + b\,n'' = 1, \tag{8}$$

where a and b are relatively prime to n'' and n', respectively. If α is a primitive nth root of unity, the field elements

$$\beta = \alpha^{bn''}; \qquad \gamma = \alpha^{an'} \tag{9}$$

[2] See any text on algebra, such as van der Waerden (1949, 1950).

are primitive n'th and n''th roots of unity, respectively. Now, since the above defined β_i and γ_i are n'th and n''th roots of unity, we may write

$$\beta_i = \beta^{\mu_i}; \qquad \gamma_i = \gamma^{\nu_i} \tag{10}$$

for some powers μ_i and ν_i. Consider the entry (i, j) of the matrix (5), with $i = r\,i'' + i'$ and $j = n'\,j'' + j'$. According to (10), this entry may be written in the form

$$h_{i,j} = (\gamma_{i''})^{j''}\,(\beta_{i'})^{j'}$$

$$h_{i,j} = (\gamma^{\nu_{i''}})^{j''}\,(\beta^{\mu_{i'}})^{j'}$$

and, using (8) and (9),

$$h_{i,j} = (\alpha^{\lambda_i})^{kj} \tag{11}$$

with

$$\lambda_i = \mu_{i'}(bn'') + \nu_{i''}\,(an') \pmod{n} \tag{12}$$

$$k_j = j'(bn'') + j''\,(an') \pmod{n} \tag{13}$$

so that the elements of row $i = r\,i'' + i'$ are in some order the first n powers of

$$\alpha^{\lambda_i} = \beta^{\mu_i}\,\gamma^{\nu_i}. \tag{14}$$

[The derivation of (11) from (12) and (13) is easily verified using the fact that an' and bn'' are mutually orthogonal idem-potents in the ring of integers modulo n.]

We now show that the rs distinct α^{λ_i}, corresponding to the rs rows of the matrix (5), are roots of distinct irreducible factors of $(x^n - 1)$ over $GF(q)$. For, suppose we would have

$$\lambda_{i_1} = q^v\,\lambda_{i_2} \pmod{n}$$

for some power v of q; this implies, using (12),

$$\mu_{i_1'} = q^v\,\mu_{i_2'} \pmod{n'},$$

which is impossible since the β^{μ_i} are roots of distinct irreducible factors $g_i(x)$ over $GF(q)$. Consequently, the code C of block length n over $GF(q)$ is equivalent, under the permutation of coordinates (j, k_j), to the cyclic code generated by the product of the minimum functions[1] of the rs roots (14). Since each factor has at most degree mp, the number of parity check digits is at most $rsmp$. Q.E.D.

Example. Let C' be the (7.1) cyclic code over $GF(2)$, generated by

TABLE I

ILLUSTRATION OF THE PERMUTATION (j, k_j) FOR $n' = 7$, $n'' = 9$, i.e., $j = 7j'' + j'$, $k_j = 36j' + 28j''$ (mod 63)

j'' \ j'	0	1	2	3	4	5	6
0	0	36	9	45	18	54	27
1	28	1	37	10	46	19	55
2	56	29	2	38	11	47	20
3	21	57	30	3	39	12	48
4	49	22	58	31	4	40	13
5	14	50	23	59	32	5	41
6	42	15	51	24	60	33	6
7	7	43	16	52	25	61	34
8	35	8	44	17	53	26	62

$g(x) = (1 + x + x^3)(1 + x^2 + x^3)$ whose roots are elements of $GF(2^3)$, and let C'' be the (9,5) cyclic code over $GF(2^3)$ generated by $G(x) = (1 + x + x^2)(1 + \beta x + x^2)$, where β is a primitive root in $GF(2^3)$. The corresponding parity check matrices may be taken as

$$H' = \begin{vmatrix} 1 & \beta & \beta^2 & \beta^3 & \beta^4 & \beta^5 & \beta^6 \\ 1 & \beta^3 & \beta^6 & \beta^2 & \beta^5 & \beta & \beta^4 \end{vmatrix},$$

where β is a primitive 7th root of unity, and

$$H'' = \begin{vmatrix} 1 & \gamma^3 & \gamma^6 & 1 & \gamma^3 & \gamma^6 & 1 & \gamma^3 & \gamma^6 \\ 1 & \gamma^4 & \gamma^8 & \gamma^3 & \gamma^7 & \gamma^2 & \gamma^6 & \gamma^1 & \gamma^5 \end{vmatrix}$$

where γ is a primitive 9th root of unity. The matrix $H = H'' \times H'$ will then be of order 4×63 over $GF(2^6)$. If α is a primitive 63th root of unity, we may write

$$\beta = \alpha^{36} \quad \text{and} \quad \gamma = \alpha^{-35} = \alpha^{28},$$

and the four rows of H will contain the 63 distinct powers of

$$\gamma^3\beta = \alpha^{57}, \qquad \gamma^3\beta^3 = \alpha^3, \qquad \gamma^4\beta = \alpha^{22}, \quad \text{and} \quad \gamma^4\beta^3 = \alpha^{31},$$

the successive powers appearing in the order of the successive rows of Table I. e.g., the 15th power appears in the $j' = 1$st position of the $j'' = 6$th sub-block. The code C is thus equivalent, under the permuta-

tion illustrated in Table I, to the cyclic code of block length 63 over $GF(2)$ generated by the product of the minimum functions of α^{57}, α^{3}, α^{22}, and α^{31}, i.e.,

$$(1 + x + x^2 + x^4 + x^6)\ (1 + x^2 + x^4 + x^5 + x^6)$$
$$\cdot (1 + x + x^3 + x^4 + x^6)\ (1 + x + x^6).$$

This code has thus $6 \times 4 = 24$ parity check digits, and can locate up to 2 erroneous subwords, each word containing not more than 6 errors. The code C' is indeed 6-error detecting, while C'' is 2-error correcting over $GF(2^3)$, as may be proved using the Bose-Chaudhuri argument [Bose and Chaudhuri (1960)], since γ^3, γ^4, γ^5, and γ^6 are roots of its generating factor.

A GENERAL DECODING PROCEDURE

The following decoding procedure requires only slight modifications of the known decoding procedure for the t-error-correcting code C'' over $GF(q^m)$.

The syndrome has rs components like (6) over $GF(q^{mp})$. These are partitioned into r subsets of s components, each subset corresponding to a distinct $\beta_{i'}$. If not more than t subwords are corrupted by error, then each subset corresponds to at most t nonzero $v_{jk}\ (\beta_{i'})$, and may thus be decoded according to the decoding procedure for the code C''. The erroneous patterns calculated from each of the r subsyndromes may be slightly different, since the $v_{jk}(\beta_{i'})$ may be zero for some i', but their union must give the correct answer. If the union contains more than t erroneous subwords, then certainly more than t errors occurred and there is some chance that the answer is not correct. This method thus permits occasional detection when more than t subwords were corrupted by errors.

Example. The decoding procedure will be illustrated for the above described EL code (63, 39) over $GF(2)$. Suppose errors occurred in the subwords of index 3 and 5, the respective error patterns being described by $1 + x + x^2$ and $1 + x^3 + x^4 + x^5$, respectively. The first component of the syndrome is then

$$\begin{aligned} S_1 &= (\gamma^3)^3(1 + \beta + \beta^2) + (\gamma^3)^5(1 + \beta^3 + \beta^4 + \beta^5) \\ &= 1\beta^5 + \gamma^6\beta^3 \\ &= \alpha^{54} + \alpha^{24}; \end{aligned}$$

and, similarly, the other components become

$$S_2 = \alpha^{54} + 0$$
$$S_3 = \alpha^{12} + \alpha^{38}$$
$$S_4 = \alpha^{12} + 0.$$

The components are then partitioned into 2 subsets. The first, corresponding to β, is (S_1, S_3) while the second, corresponding to β^3, is (S_2, S_4). Each of these subsyndromes is decoded as a syndrome for the code C''. This can be done using the procedure described in Peterson (1961) and gives as erroneous patterns:

subwords of index (3, 5) for (S_1, S_3)

subword of index (3) for (S_2, S_4).

Their union gives (3, 5), which contains not more than 2 erroneous subwords and may thus be regarded as the correct answer.

We emphasize that the syndrome may be calculated directly, using the parity check matrix of the equivalent cyclic code, if the coordinates are rearranged to appear in their natural order. For instance, the error pattern described for the above example may be expressed, in terms of the coordinates of the equivalent cyclic code, as

$$e(x) = x^{21}(1 + x^{36} + x^{9}) + x^{14}(1 + x^{45} + x^{18} + x^{54}),$$

and the first component of the syndrome is calculated as

$$e(\alpha^{57}) = \alpha^{54} + \alpha^{24}.$$

CONNECTIONS WITH SOME PREVIOUSLY CONSIDERED EL CODES

Single sub-block error-locating codes were first considered by Wolf and Elspas (1963). These codes have block length $n = (t + 1)^m - 1$ and $r = m\rho$ check digits and are constructed by means of a $(t, t - \rho)$ cyclic code over $GF(2)$. The case $t = 2^\rho - 1$ was considered by these authors, and they noted that the resulting EL codes are optimum. It is not difficult to see that the codes obtained are equivalent to ours by setting

$$C' = (2^\rho - 1, 2^\rho - 1 - \rho) \text{ over } GF(2) \tag{15}$$

$$C'' = \left(\frac{2^{m\rho} - 1}{2^\rho - 1}, \frac{2^{m\rho} - 1}{2^\rho - 1} - m\right) \text{over } GF(2^\rho). \tag{16}$$

Note that C' is a perfect binary Hamming code, while C'' is a generalized

Hamming code, provided $(2^{m\rho} - 1)/(2^{\rho} - 1)$ and $(2^{\rho} - 1)$ are relatively prime.

A second family was considered by Wolf and Elspas, leading to nonoptimum codes, but the authors noted that it is possible in some cases to extend these codes, and this point has been somewhat clarified by Wolf (1965). An equivalent family of cyclic error-locating codes may be obtained by setting

$$C' = (t, t - \rho) \text{ over } GF(2),$$

with $2^{\rho} - 1 = kt$, and C'' as in (16), the resulting EL code being equivalent to a cyclic code of block length

$$n = \left(\frac{2^{m\rho} - 1}{2^{\rho} - 1}\right) t$$

with $r = m\rho$ parity check digits.

Finally, a subclass of the multiple sub-block EL codes considered by Wolf (1965) is equivalent to a class of cyclic error locating codes. This class is obtained by setting

$$C' = (t, t - \rho) \text{ over } GF(2)$$

with

$$(2^{\rho} - 1) = kt \quad \text{and} \quad C'' = (s, s - m) \text{ over } GF(2^{\rho}),$$

with s relatively prime to t. The resulting error-locating code will have block length $n = st$ and $r = m\rho$ check digits.

RECEIVED: August 5, 1966

REFERENCES

BOSE, R. C., AND RAY-CHAUDHURI, D. K. (1960). On a class of error-correcting binary group codes. *Information and Control* **3**, 68–79.

BURTON, H. O., AND WELDON, E. J. (1965). Cyclic product codes. *IEEE Trans. Information Theory, I.T.-11* **3**, 433–440.

CHANG, S. H., AND WENG, L. J. (1965). Error-locating codes. *IEEE Intern. Convention Rec.* Part **7**, 252–258.

PETERSON, W. W. (1961). "Error Correcting Codes." M.I.T. Press, Cambridge, Massachusetts.

VAN DER WAERDEN, B. L. (1949, 1950). "Modern Algebra" (2 volumes), translated by F. Blum and T. J. Benac. Fred. Ungar, New York.

WOLF, J. K. (1965). On an extended class of error-locating codes. *Information and Control* **8**, 163–169.

WOLF, J. K., AND ELSPAS, B. (1963). Error-locating codes—a new concept in error control. *IEEE Trans. Information Theory, I.T.-9* **2**, 113–117.